SVC: Switched Virtual Circuit.

TCP: Transmission Control Protocol.

TDMA: Time Division Multiple Access, one of several wireless access methods.

telecommunication service provider[1] **(TSP):** defined from CALEA Section 102 (8) to be, "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, and includes 1) a person or entity engaged in providing commercial mobile service, or 2) a person or entity engaged in providing wire or electronic communications switching or transmission service to the extent that the Commission finds such service is a replacement for a substantial portion of local telephone exchange service and that it is in the public interest to deem such a person or entity to be a [TSP] for purposes of this title. This does not include 1) persons or entities insofar as they are engaged in providing information services, and 2) any class or category of [TSPs] that the Commission exempts by rule after consultation with the U. S. Attorney General."

telecommunication support services: defined in CALEA Section 102 (7) to be "a product, software, or service used by a [TSP] for the internal signaling or switching functions of its telecommunication network."

terminal mobility: the ability of a terminal to access telecommunications services from different locations and while in motion, and the capability of the network to identify, locate, and communicate with that terminal. Terminal mobility while not on a call may involve *roaming*, or while on a call may involve *handoff.*

termination: an incoming call attempt. see also call-identifying information.

transmission: the act of transferring communications from one location or another by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.

transparent: end-to-end transmission without insertion or loss of information.

trap and trace device: defined in 18 USC 3127 (4) to be "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."

TSP: telecommunication service provider.

unobtrusive: not undesirably noticeable or blatant; inconspicuous; within normal call variances.

URL: Uniform Resource Locator.

USC: United States Code.

[1] This Standard uses the term *telecommunication service provider* instead of the CALEA term *telecommunication carrier*.

user-to-user signaling: a bi-directional packet-mode data service for wireline subscribers.

UTC: Coordinated Universal Time (as defined by the CCIR (ITU-R)).

virtual circuit: a packet-mode connection between two end-points. A virtual circuit may be *permanent* (with only a data transfer phase) or *switched* (with setup, data transfer, and release phases).

WCDMA: Wideband Code Division Multiple Access, one of several wireless access methods.

wire communications: defined in 18, USC 2510 (1) to be "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication."

wireless: refers to cellular or personal communication service (PCS).

wireline: refers to traditional wire-based telephone service.

4 Stage 1 Description: User Perspective

This section describes the features and services of LAES from a user's perspective. In this case the user is the LEA and its monitoring equipment. The features and services are described with enough detail to let LEAs know what information can be collected and when it can be collected.

4.1 Overview

This Standard defines the means to access communications as an intercept access service. The services fall into three categories:

- non-call associated services to provide information about intercept subjects that is not necessarily related to a call (see 4.3);
- call associated services to provide call-identifying information about calls involving the intercept subjects (see 4.4); and
- content surveillance services to provide access to an intercept subject's communications (see 4.5).

Restrictions are defined for exceptions (see 4.6).

4.2 Introduction

4.2.1 Assumptions

LAES capabilities allow a TSP to deliver the intercepted call content (e.g., voice, packet data, modem data) and call-identifying information to an authorized LEA.

Content: is defined in 18 USC 2510 (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."

Call-identifying information: is defined in CALEA Section 102 (2) to be "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a [TSP]." As interpreted by this Standard: *destination* is the number of the party to which a call is being made (e.g., called party); *direction* is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); *origin* is the number of the party initiating a call (e.g., calling party); and *termination* is the number of the party ultimately receiving a call (e.g., answering party).

Call-identifying information is *reasonably available* if the information is present at the Intercept Access Point (IAP) for call processing purposes. Network protocols (except LAESP) do not need to be modified solely for the purpose of passing call-identifying information. The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves.

The terms *call content* and *call-identifying information* are used throughout this Standard. The term *call* in this Standard is intended to be used in a generic sense to denote a communication and is not limited to circuit-mode or connection-oriented communications.

Not all information delivered to law enforcement is call-identifying information or call content.

Call identities are used to correlate call-identifying information and call content.

4.2.2 General Background

The intercept function is viewed as four broad categories: access, delivery, collection, and administration. These functions are discussed functionally without regard to their implementation. The relationships between these functional categories are shown in Figure 1.

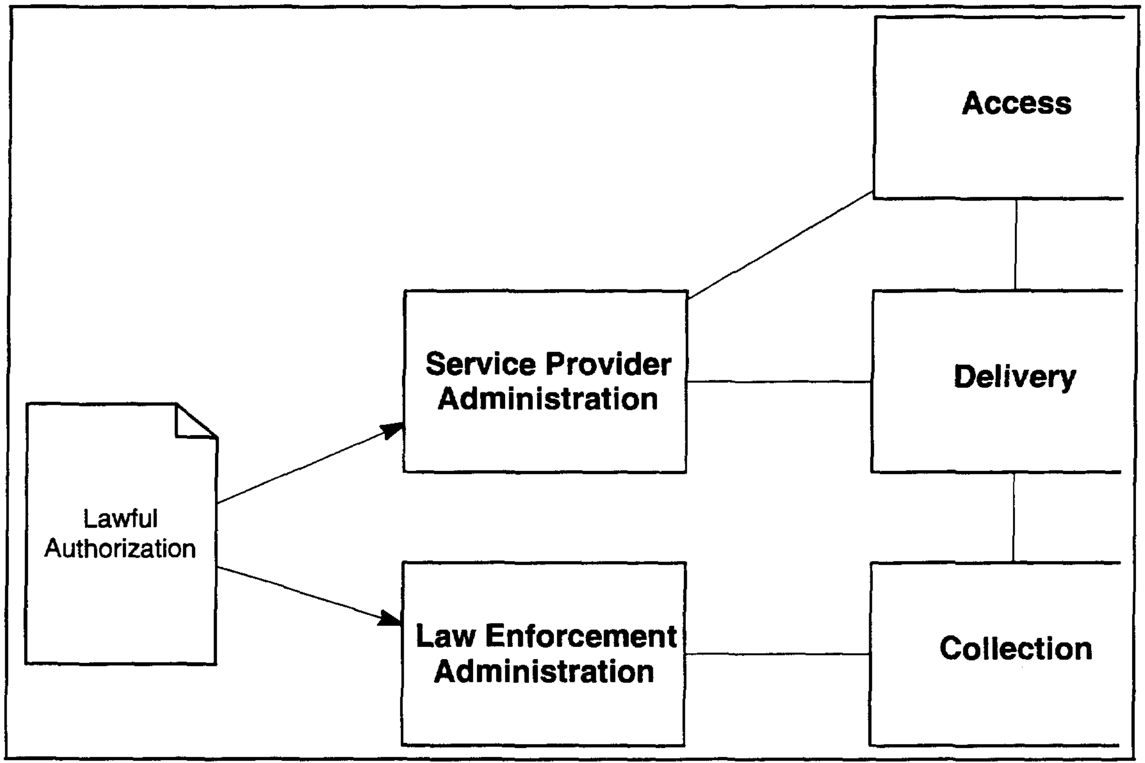
Access
Service Provider Administration
Delivery
Lawful Authorization
Law Enforcement Administration
Collection

Figure 1: **Electronic Surveillance Model**

The Access Function, consisting of one or more Intercept Access Points (IAPs), isolates an intercept subject's communications or call-identifying information unobtrusively. The IAPs may vary between TSPs and may not be available on all systems.

The Delivery Function is responsible for delivering intercepted communications to one or more Collection Functions. The Delivery Function delivers information over two distinct types of channels: Call Content Channels

(CCCs) and Call Data Channels (CDCs). The CCCs are generally used to transport call content, such as voice or data communications. The CDCs are generally used to transport messages which report call-identifying information, such as the calling party identities and called party identities.

The Collection Function is responsible for collecting and analyzing intercepted communications and call-identifying information. The Collection Function is the responsibility of the LEA.

The Service Provider Administration Function is responsible for controlling the TSP Access and Delivery Functions.

The Law Enforcement Administration Function is responsible for controlling the LEA Collection Function.

The lawful authorization, while neither a network entity nor an interface reference point, is an important part of LAES. No intercepts shall take place without specific lawful authorization.

4.2.3 Call Content Channels and Call Data Channels

A TSP is required to provide access to the communications and call-identifying information for particular intercept subjects.

A subject's call content is generally transported to the LEA over one or more CCCs. The actual number of CCCs will vary with each electronic surveillance according to the number of CCCs ordered by the LEA. Factors influencing this number are the subject's bearer capabilities, the subject's call capabilities, the type of communication being intercepted, the type and capacity of individual CCCs, the number of possible call appearances, and the subject's call-related activities. CCCs shall be provisioned as *combined* (i.e., carrying both the transmit and receive paths on one channel) or *separated* (i.e., using independent channels for the transmit and receive paths). Each CCC for an electronic surveillance must be capable of transporting one or more of the subject's intercepted bearer services. For some types of applications used by the subject (e.g., short message service), the call content may be transported over the CDC.

Additional CCCs shall be used (up to the number provisioned for a particular electronic surveillance) when the CCCs currently open are incompatible with the bearer services being intercepted. An example of this situation could be when a subject initiates a voice call, optionally places that call on hold, and initiates a second call using a different bearer service (e.g., fax or data).

The type of CCC delivered to an LEA may be influenced by the subject's bearer services, the manner in which the subject's call content is accessed, the preferences of the TSP, and the preferences of the LEA conducting the electronic surveillance. Communications that inherently use separate transmit and receive communications paths require separated CCCs. Other communications inherently combine the transmit and receive paths (or assume that the paths may be combined), so combined CCCs may be appropriate.

Call-identifying information is formatted into discrete messages using a specialized protocol called the Lawfully Authorized Electronic Surveillance Protocol (LAESP). The LAESP messages shall be transported to an LEA over a CDC. As defined in this Standard, a single CDC may support the delivery of LAESP messages for one or more electronic surveillances to a particular LEA collection facility.

The CDCs and CCCs shall use separate logical channels as shown in Figure 2. The CDC and CCC(s) may be transported to an LEA over separate or common physical facilities. The CDCs may be multiplexed onto one or more physical facilities.

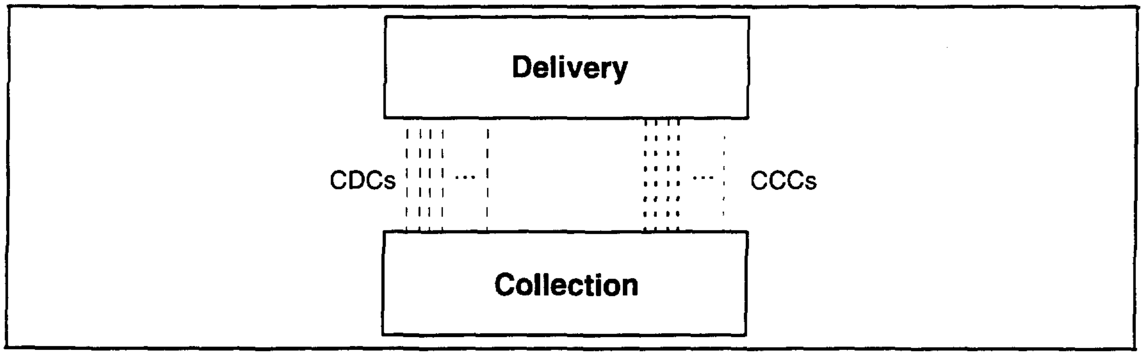

Figure 2: **Call Content Channels and Call Data Channels**

Rare circumstances dictate that the call-identifying information, call content, or both associated with a particular subject need to be delivered to more than one LEA Collection Function simultaneously. This will occur when different LEAs are conducting independent investigations on the same subject. The Delivery Function shall duplicate the call content, call-identifying information, or both and deliver only authorized information. No more than five Collection Functions need to be supported for any single intercept subject. Separate circuits should be used to deliver the call content and call-identifying information to each LEA. The delivery options may be different for each path between an Access Function and a Collection Function.

Each CCC has a unique identity that is mutually agreed upon by the TSP and the LEA. The identity may be for a particular dedicated nailed up circuit, a dynamically allocated trunk member, or a directory number used for a switched connection. Each CCC may use a variety of physical implementations between the TSP and the LEA, but each CCC shall be uniquely identified.

4.3 Non-Call Associated Information Surveillance Service Description—Serving System IAP

Non-call associated information surveillance services access information within telecommunication systems. Information may be retrieved from existing messages and signaling or it may be derived from other information.

The Serving System Identification IAP (SSIAP) is the only non-call associated information IAP identified. The SSIAP shall report with a ServingSystem message the identification of the TSP providing service to a subject using a terminal or personal mobility service.

The serving system identification information includes the identity of the current system assigned to provide service for the mobile. Information regarding the occurrence of the event (e.g., identification of the system providing the intercept access, time, date) should be included. In some situations the Serving System may be identified with a directory number (e.g., when a mobile station registers to a personal base station).

4.4 Call Associated Information Surveillance Service Description—Call-Identifying Information IAP

Call associated information surveillance services access information pertaining to call and service processing. This may span several functional entities.

The Call-Identifying Information IAP (IDIAP) is the only call associated information IAP identified. It provides expeditious access to the reasonably available call-identifying information for calls made by an intercept subject or for calls made to an intercept subject. This includes abandoned and incomplete call attempts and calls that are redirected (e.g., diverted, forwarded, or deflected) by any party of the call.

A call event is a user action or signal that may cause a call state change. These events are not intended to reflect a particular technology, but to describe the event in general.

The IAP shall access the call-identifying information for the intercept subject unobtrusively. Access to call-identifying information shall not deny the availability of any service to either the subject or associates.

The following call events are defined for circuit-mode calls only:

Answer

A party has answered the call attempt.

Change

The identity of a call has been merged with the identity(ies) of other call(s) or split into multiple call identities.

Origination

The system has routed a call dialed by the subject or the system has translated a number for the subject.

Redirection

A call has been redirected (e.g., forwarded, diverted, or deflected).

Release

The facilities for the entire call have been released.

TerminationAttempt

A call attempt to an intercept subject has been detected.

4.5 Content Surveillance Service Description

The IAPs for content surveillance are used to access the communications of an intercept subject. The content extracted by a content surveillance IAP shall be delivered over a CCC or CDC. The IAPs may be dynamically added or dropped as necessary to access the communications of the intercept subject.

The following categories of content IAPs have been defined:

- Circuit IAP
- Packet Data IAP

The IAPs for content surveillance shall access the transmissions to and from the intercept subject unobtrusively. Access to call content shall not deny the availability of any service to either the subject or associates.

Content surveillance services provide access to calls at the IAP. Abandoned or incomplete calls may also be accessed.

Loss of any portion (i.e., the beginning, middle, or end) of call content should not occur.

A TSP shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the TSP and the TSP possesses the information necessary to decrypt the communication.

The call-identifying information associated with the circuit-mode content surveillance is provided on the CDC by an IDIAP.

4.5.1 Circuit IAP

The Circuit IAP (CIAP) shall access the call content of circuit-mode communications to or from the equipment, facilities, or services of an intercept subject. This may include incoming calls to an intercept subject before they are answered and calls to an intercept subject that are redirected to another party. This may include call progress tones or announcements.

Multiple CIAPs may be necessary for intercept subjects with multiple terminals or for terminals or services supporting multiple call appearances.

An idle CCC shall be selected from the CCCs available for this intercept subject and the selected destination. The selection criteria should use all CCCs on a regular basis.

Figure 3 shows the basic CIAP to access a two-way communication. [1]

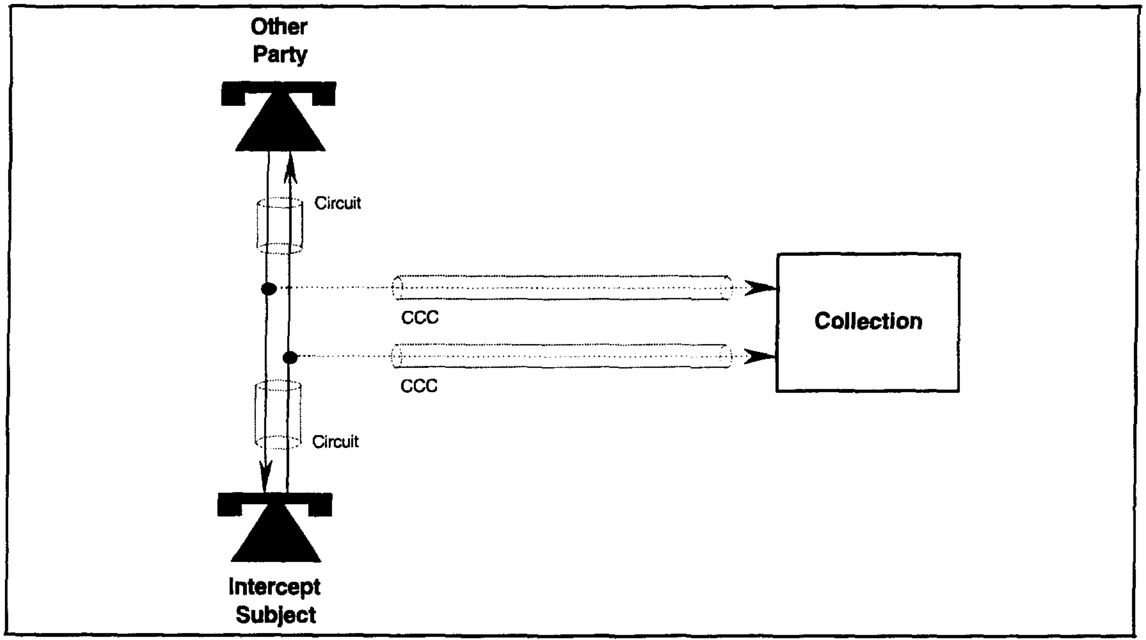

Figure 3: **Circuit IAP for a Two-Way Communication**

[1] The symbols used in Figure 3 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

The Circuit IAP (CIAP) shall access a multi-party circuit-mode communication (e.g., Three-Way Calling, Conference Calling, or Meet Me Conferences) as it would be presented to the intercept subject. This is depicted in Figure 4.[1]

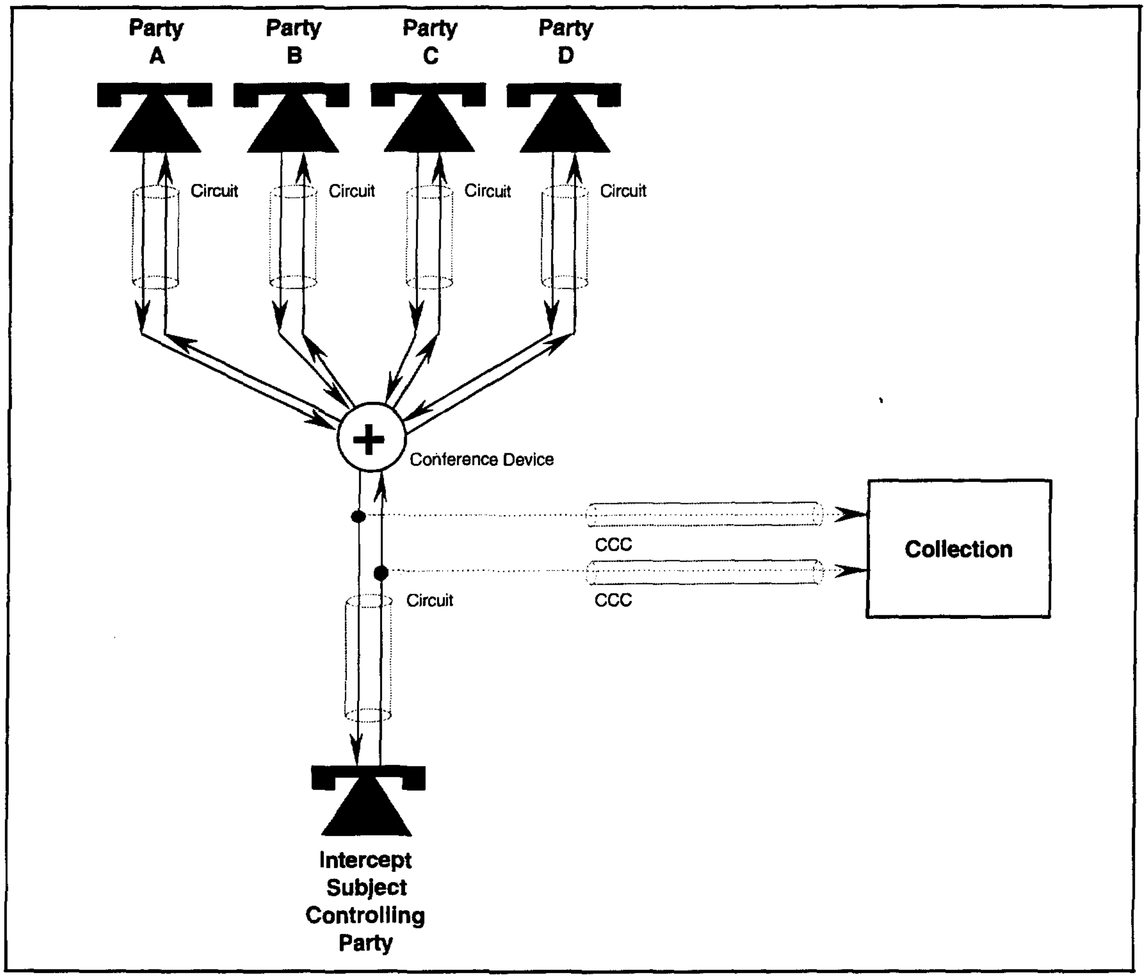

Figure 4: **Circuit IAP for a Multi-Party Communication**

[1] The symbols used in Figure 4 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

The CIAP may access a call to the intercept subject before the intercept subject answers, as shown in Figure 5. This may provide access to call progress tones or announcements played toward the calling party. Normally the calling party is not cut-through and is not accessible until the call is answered. This access may be independent of the intercept subject, in that the intercept subject may be engaged in other services or communicating with other parties while the incoming call is accessed. [1]

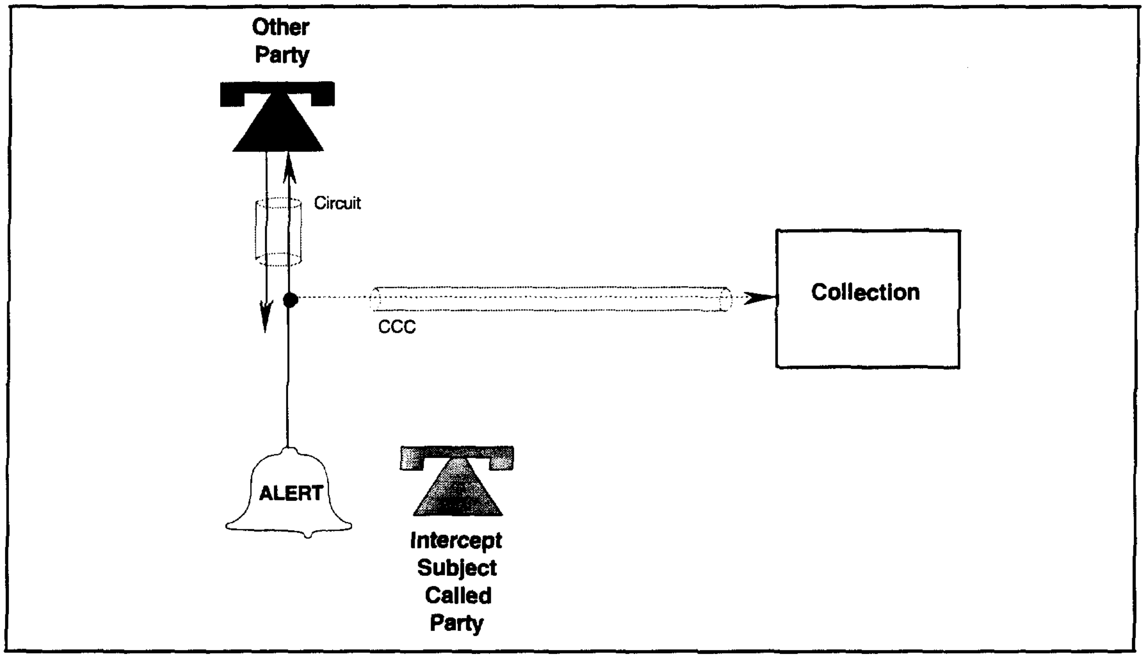

Figure 5: **Circuit IAP for an Incoming Call**

If the call is answered for user interaction; (e.g., to request a personal identification number (PIN), password, or extension number), both communication paths should be accessed.

[1] The symbols used in Figure 5 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

The CIAP shall access a call redirected by the intercept subject. Redirection includes any rerouting of a call, for example, call delivery, call forwarding, call deflection, or call diversion. This access is independent of the intercept subject, as the intercept subject may engage in another communication or service at any time while a redirected call is in progress as shown in Figure 6.[1]

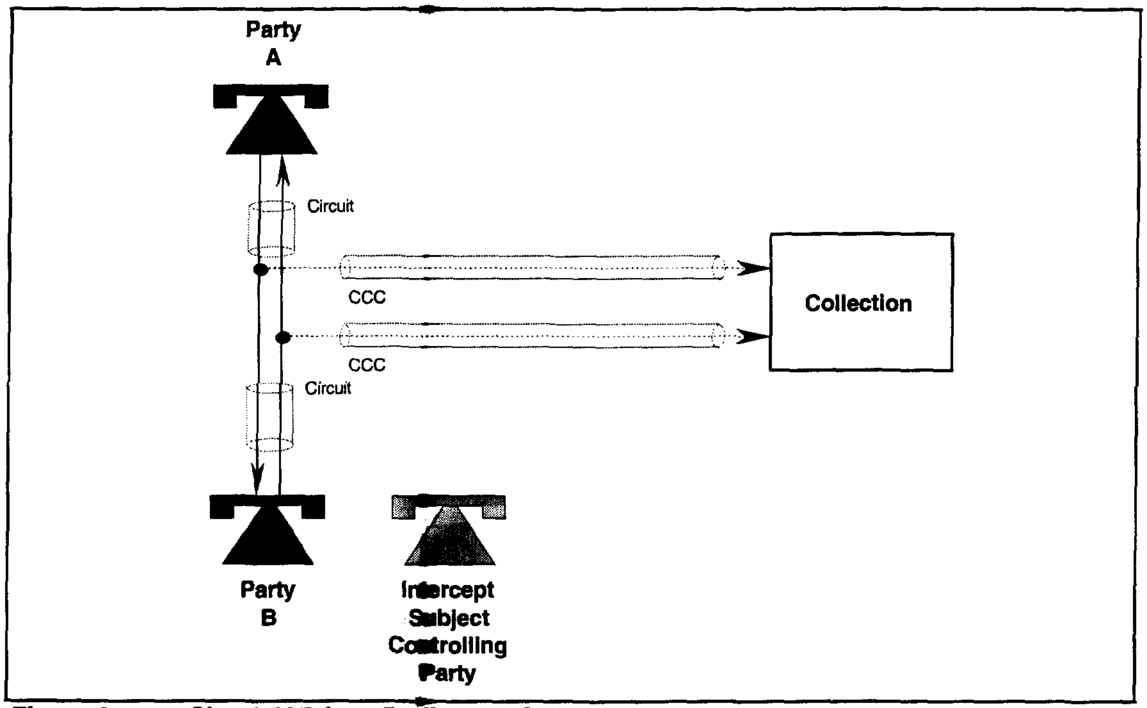

Figure 6: **Circuit IAP for a Redirected Call**

4.5.2 Packet Data IAP

A Packet Data IAP (PDIAP) shall access data packets sent or received by the equipment, facilities. or services of an intercept subject when a packet-mode data service is provided. PDIAPs may be on the Serving System or on the Redirecting System. An IAP on the Redirecting System is only able to access some packets delivered to the intercept subject (and possibly none of the packets originated by the intercept subject).

Packets shall be sent to the Collection Function when they are intercepted. The intercepted packets shall be delivered without interpretation or modification, except for possible re-framing, segmentation, or enveloping required to transport the information to the Collection Function. The access includes all packet-mode data transmissions regardless of their outcome. For example, when an SMS packet to a Mobile Station (MS) is intercepted, it is not known whether the packet was actually received by the MS.

[1] The symbols used in Figure 6 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

A Packet Data IAP (PDIAP) provides access to one or more of the following packet-mode data services:

- ISDN user-to-user signaling,
- ISDN D-channel X.25 packet services,
- Short Message Services (SMS) for cellular and Personal Communication Services (e.g., NAMPS, *IS-41*, PCS1900, or GSM-based technologies),
- wireless packet-mode data services (e.g., Cellular Digital Packet Data (CDPD), CDMA, TDMA, PCS1900, or GSM-based packet-mode data services),
- X.25 services,
- TCP/IP services,
- paging (one-way or two-way), and
- packet-mode data services using traffic channels.

Separated CCCs may be used to transport packet data to the Collection Function as shown in Figure 7.[1]

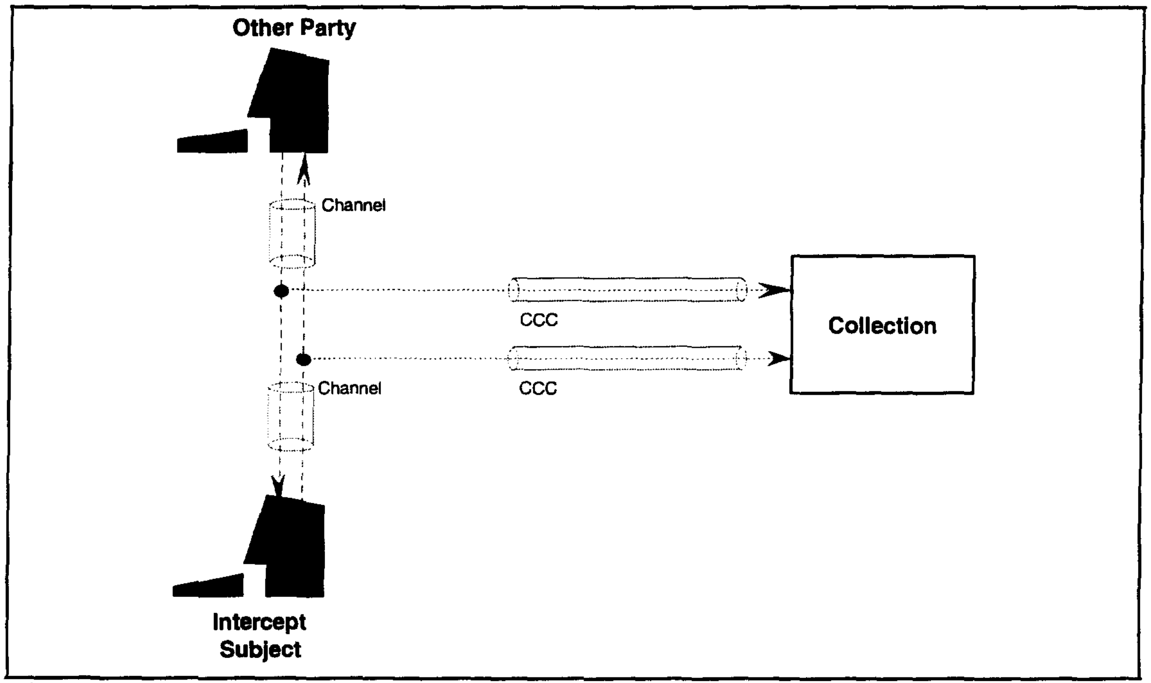

Figure 7: **Packet Data IAP to a Separated CCC (appropriate to all data services)**

[1] The symbols used in Figure 7 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

Connectionless data services may use separated delivery as shown above or they may use combined delivery as depicted in Figure 8.[1]

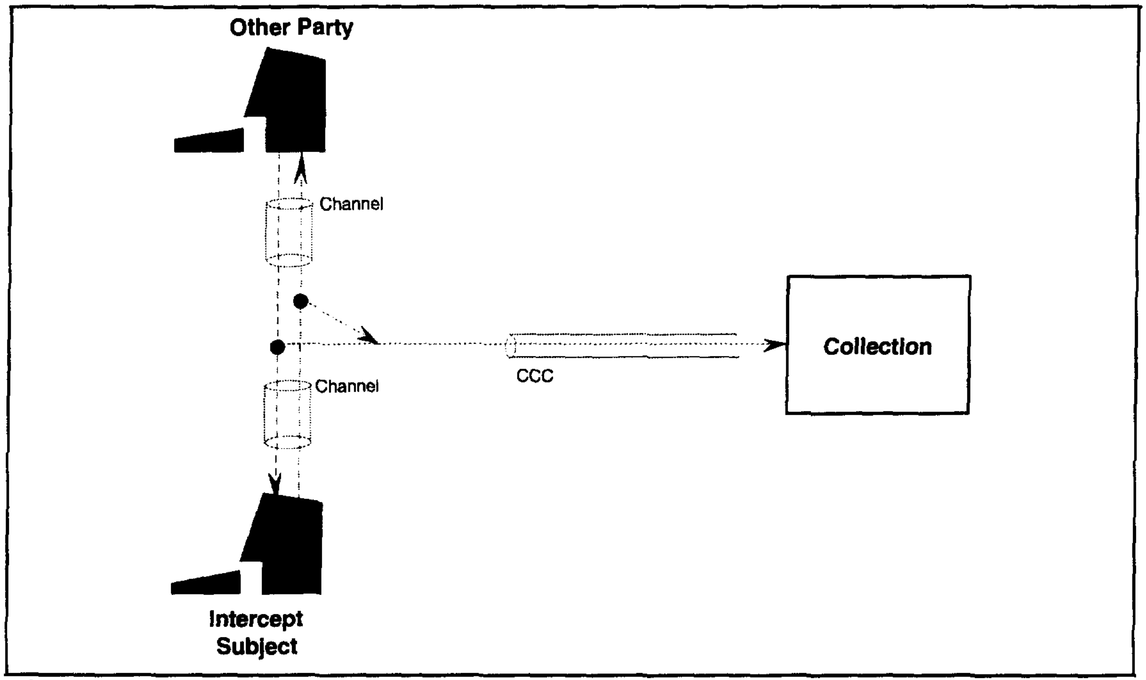

Figure 8: **Packet Data IAP to a Combined CCC (connectionless data services only)**

[1] The symbols used in Figure 8 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

Certain intercepted packets may be delivered over a CDC using PacketEnvelope messages as shown in Figure 9.[1]

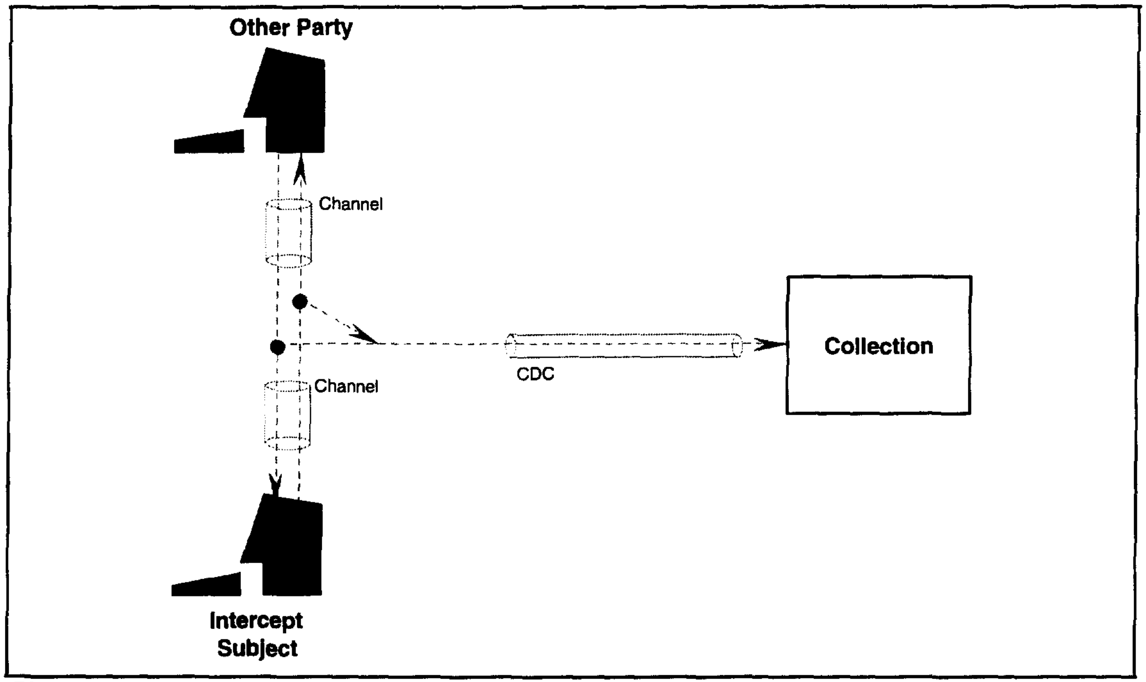

Figure 9: **Packet Data IAP to a CDC (for selected packet types)**

[1] The symbols used in Figure 9 represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

4.6 Restrictions

4.6.1 Lack of CDC and CCC Synchronization

The CDC and CCC information will not necessarily be synchronized when received by an LEA, since the call content and call-identifying information are delivered to an LEA using the independent services of the CCCs and CDCs respectively, and since the services can be provided on independent networks (e.g., dedicated circuits for the CCC and switched packet network delivery for the CDC).

4.6.2 CDC Congestion

When the call-identifying information intercept communication resources, e.g., CDCs, are limited, the communications are accessed on a first-in, first-out, non-queued basis. If a particular CDC is congested and the associated buffers (if any) are full, messages destined to that CDC may be discarded by the originating end. Unavailability or congestion of a CDC shall not affect other CCCs or CDCs.

4.6.3 CCC Exhaustion

When the call content intercept communication resources, e.g., CCCs, are limited, the communications are accessed on a first-come, first-served, non-queued basis. In other words, CCCs are assigned as they are needed. If a CCC is needed and none is available, that request is ignored, even if a CCC should subsequently become available during the communication pertaining to that request. The CCC may remain unused until the next request for a CCC for the subject is received. Unavailability of a CCC shall not affect other CCCs or CDCs.

Channels dedicated to a particular subject shall not be used for other subjects.

4.6.4 CCC Congestion

For CCCs used for packet-mode delivery, the bandwidth available depends upon the communication facilities and also upon concurrent traffic. If a packet-mode CCC toward the Collection Function becomes congested, intercepted packets may be discarded. Congestion of a CCC shall not affect other CCCs or CDCs.

5 Stage 2 Description: Network Perspective

5.1 Introduction

This section describes the information flows between the Access, Delivery, and Collection Functions to support LAES. The information flows are usually described as messages and information carried by a message.

5.2 Stage 2 Methodology

This section describes the methodology and organization for the development of the Stage 2 network perspective descriptions. A network reference model is developed and then information flows between functional entities over reference points are described.

Information is described in terms of a causing event and information associated with that event. Within each service description there is a set of events to support the particular service and a data dictionary to define a set of information elements to support the events.

Stage 2 for LAES CDCs deals with the movement of information between the Access, Delivery, and Collection Functions. The CDC Stage 2 description focuses on the information being transferred, rather than the transfer mechanism.

CCCs shall be delivered to LEAs using protocols as specified in Section 6.5.

5.3 Network Reference Model

The Network Reference model, as shown in Figure 10, consists of a set of functional entities and interface reference points between some of those functional entities. The functional entities provide the functions of the system, and an interface reference point allows information to be exchanged between the two functional entities connected by the interface reference point.

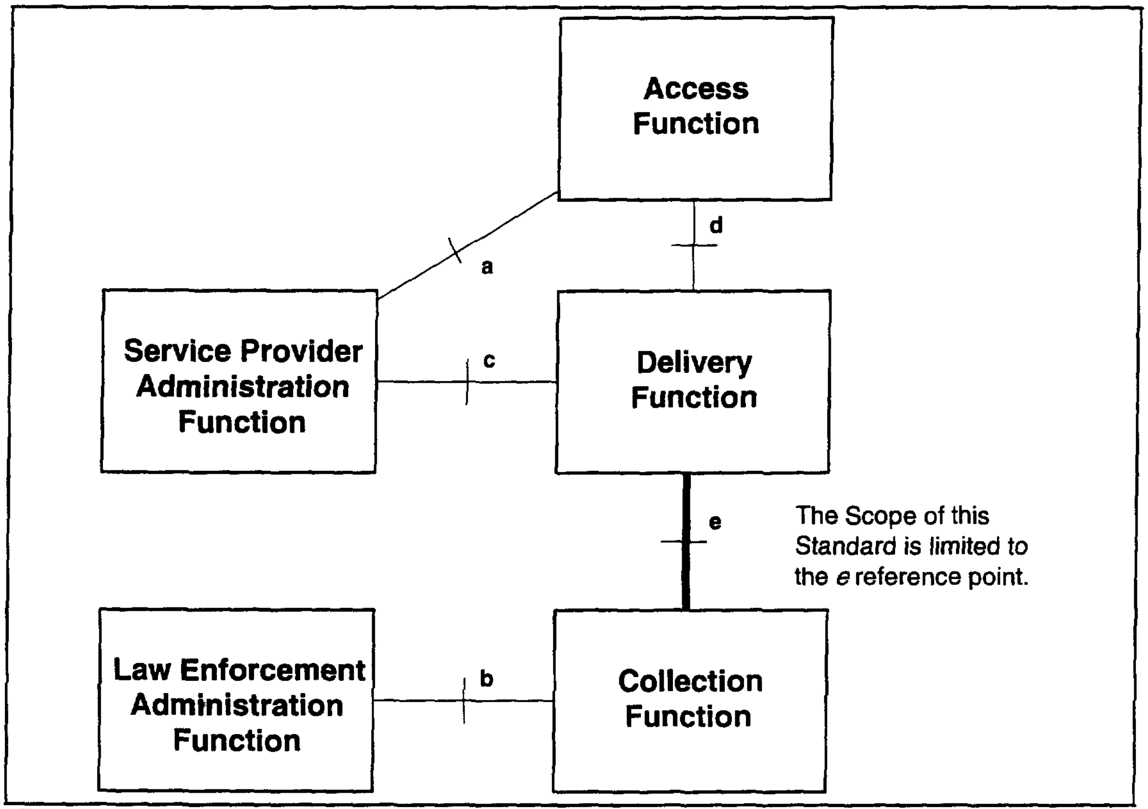
Access Function
d
a
Service Provider Administration Function
c
Delivery Function
e
The Scope of this Standard is limited to the *e* reference point.
Law Enforcement Administration Function
b
Collection Function

Figure 10: **Network Reference Model**

5.3.1 Functional Entities

5.3.1.1 Access Function (AF)

The Access Function, through its constituent Intercept Access Points (IAPs), provides access to an intercept subject's communications, call-identifying information, or both.

The Access Function typically includes the ability:

- to access intercept subject's call-identifying information unobtrusively and make the information available to the Delivery Function;
- to access intercept subject call content unobtrusively and make the call content available to the Delivery Function; and
- to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information consistent with TSP security policies and practices.

5.3.1.2 Delivery Function (DF)

The Delivery Function is responsible for delivering intercepted communications and call-identifying information to one or more Collection Functions.

The Delivery Function typically includes the ability:

- to accept call content for each intercept subject over one or more channels from the Access Function(s);
- to deliver call content for each intercept subject over one or more CCCs to a Collection Function;
- to accept call-identifying or packet-mode content information for each intercept subject over one or more channels and deliver that information to the Collection Function over one or more CDCs;
- to ensure that the call-identifying information and call content delivered to a Collection Function is authorized for a particular LEA;
- to duplicate and deliver authorized call-identifying information and content for the intercept subject to one or more Collection Functions (up to a total of five); and
- to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information consistent with TSP security policies and practices.

5.3.1.3 Collection Function (CF)

The Collection Function is responsible for collecting lawfully authorized intercepted communications (i.e., call content) and call-identifying information for an LEA.

The Collection Function typically includes the ability:

- to receive and process call content information for each intercept subject; and
- to receive and process information regarding each intercept subject (e.g., call associated or non-call associated).

The Collection Function is the responsibility of the LEA.

5.3.1.4 Service Provider Administration Function (SPAF)

The Service Provider Administration Function is responsible for controlling TSP electronic surveillance functions.

The functions of the SPAF are beyond the scope of this Standard.

5.3.1.5 Law Enforcement Administration Function (LEAF)

The Law Enforcement Administration Function is responsible for controlling LEA electronic surveillance functions.

The functions of the LEAF are beyond the scope of this Standard.

5.3.2 Interface Reference Points

5.3.2.1 Reference Point a

Reference point *a* is the interface between the Service Provider Administration Function and the Access Function.

Reference point *a* is beyond the scope of this Standard. [1]

5.3.2.2 Reference Point b

Reference point *b* is the interface between the Law Enforcement Administration Function and the Collection Function.

Reference point *b* is beyond the scope of this Standard.

5.3.2.3 Reference Point c

Reference point *c* is the interface between the Service Provider Administration Function and the Delivery Function.

Reference point *c* is beyond the scope of this Standard. [1]

5.3.2.4 Reference Point d

Reference point *d* is the interface between the Access Function and the Delivery Function.

Reference point *d* is beyond the scope of this Standard. [1]

[1] This reference point is required to protect (e.g., prevent unauthorized access, manipulation, and disclosure) 1) the privacy and security of communications and call-identifying information not authorized to be intercepted; and 2) information regarding the government's interception of communications and access to call-identifying information.

5.3.2.5 Reference Point e

Reference point *e* is the interface between the Delivery Function and the Collection Function.

Reference point *e* is defined by this Standard.[1]

5.4 Message Descriptions

The simple call events described in Stage 1 convey the basic information for reporting the disposition of a call. This section describes those events and supporting information.

Each message is described as consisting of a set of parameters. Each parameter is either mandatory (M)—required for the message, conditional (C)—required in situations where a condition (defined in the usage column of the table) is met, or optional (O)—provided at the discretion of the implementation. The information to be carried by each parameter is identified. Please note that both optional and conditional parameters at Stage 2 are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion requirements take precedence over the Stage 3 syntax.

5.4.1 Answer

The Answer message reports when a circuit-mode call or call leg has been answered. Transmission is usually cut-through in both directions to the intercept subject or its agent.

The Answer message shall be triggered when:

- the intercept subject answers a call or call leg that has not been previously answered by the intercept subject;
- an agent of the intercept subject (e.g., by voice mail or for password screening) answers a call or call leg;
- an associate answers an outgoing call from the intercept subject as detected by the accessing functional entity;
- a call redirected by the intercept subject is answered as detected by the accessing functional entity; or
- the intercept subject or its agent answers a recalling associate (e.g., hold recall, transfer recall, or attendant recall).

The Answer message includes the following parameters:

Table 1: **Answer Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call within a system.
Answering PartyIdentity	C	Include, when known, to identify the answering party or agent.
Location	C	Include, when a terminating call is answered, the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
BearerCapability	C	Include, when known (or presumed), to indicate the granted bearer service.

See 6.3.1 "Answer Message" on page 44 for the Stage 3 description.

5.4.2 CCClose

The CCClose message reports the end of call content delivery.

The CCClose message shall be triggered when the CCC is released, such as when:

- the intercepted circuit-mode call is released;
- the intercepted circuit-mode call leg is released;
- the intercepted circuit-mode call is merged with another intercepted circuit-mode call; or
- the intercepted circuit-mode call leg is merged into another intercepted circuit-mode call.

The CCClose message may be triggered when:

- an early release of the circuit-mode or packet-mode CCC by the Collection Function or intervening network is detected (e.g., see B.3.7);
- a delivery channel for packet data is no longer required; or
- the monitored packet-mode call is released.

One CCClose message is required for each delivered combined CCC, separated CCC pair, or individual CCC.

The CCClose message includes the following parameters:

Table 2: **CCClose Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Include for circuit-mode calls to identify a particular call instance for the CCC.
CCCIdentity	M	Identifies the CCC(s) used to deliver a particular call leg (e.g., a trunk identity, telephone number, or a data network address).

See 6.3.2 "CCClose Message" on page 45 for the Stage 3 description.

5.4.3 CCOpen

The CCOpen message associates a circuit-mode CCC with a particular call instance.

The CCOpen message shall be triggered when circuit-mode call content delivery begins. This should occur after a call is initiated (as an intercept subject origination or termination attempt), but prior to the cut-through of communications between the subject and associate (usually indicated with an answer).

The CCOpen message may be triggered when a delivery CCC is required for packet-mode data. The CCOpen is required when intercepted packets are to be delivered over a circuit or over a packet switched data network. Packet-mode delivery uses a single packet data network service to deliver intercepted packets to a single address per Collection Function. Packet-mode delivery is differentiated from a circuit-mode intercept by including a PDUType parameter instead of a CallIdentity parameter. Circuit-mode delivery CCCs may deliver packet-mode contents as identified by the BearerCapability parameter or by an agreement between the TSP and LEA.

One CCOpen message is required for each delivered combined CCC, separated CCC pair, or individual CCC.

The CCOpen message includes the following parameters:

Table 3: **CCOpen Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
ContentType One of:	M	
CallIdentity		Include for circuit-mode calls to identify a particular circuit-mode call instance for the CCC. A unique call identity may be generated for the CCOpen message which is used to correlate other messages with the delivered call content.
PDUType		Include for packet-mode calls to identify the type of packet data units being intercepted (e.g., IP, PPP, X.25 LAPB, ISDN D-channel).
CCCIdentity	M	Identifies the CCC(s) used to deliver a particular call leg (e.g., a trunk identity, telephone number, or a data network address).

See 6.3.3 "CCOpen Message" on page 45 for the Stage 3 description.

5.4.4 Change

The Change message reports a change in circuit-mode call identity, especially when merging or splitting call identities.

The Change message shall be triggered when:

- two or more call identities are merged into one call identity;
- a call identity is split into two or more call identities; or
- a call identity is changed to another call identity.

The Change message includes the following parameters:

Table 4: **Change Message Parameters**

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
Previous CallIdentity	M	Identifies the call identities previously used in messages. Any call identity that was previously used but is not mentioned as a resulting call identity is released and may be reassigned to other calls.
Resulting Calls	M	Identifies the CallIdentity(ies) and CCCIdentity(ies) in the resulting calls. New unique call identities may be generated for the Change message which is used to correlate subsequent messages with the delivered call content.

See 6.3.4 “Change Message” on page 45 for the Stage 3 description.

5.4.5 Origination

The Origination message reports circuit-mode call origination attempts or number translations for the intercept subject. More than one Origination message is possible for a single call attempt when numbers are expanded or translated.